Marriage • Parenting • Spiritual Growth • Sexuality • Relationships • Mental Health
Men • Women • Hurts and Emotions • Singles • Ministers and Mentors • Technology

Technology Guidelines For Christian Business Owners

APOSTOLIC CHRISTIAN
Counseling and Family Services
Helping the hurting. Nurturing hope. Encouraging growth.
Phone: (309) 263-5536 | www.accounseling.org

Technology Guidelines For Christian Business Owners

Christian business owners and employers have a unique opportunity and responsibility to model godly behavior to their employees and customers through appropriate technology use. It is encouraged employers consider protecting their employees as diligently as they would protect their own families. Staying informed of potential risks and taking proactive steps to minimize these risks can help provide a safe and productive technology environment for themselves and their employees.

Scriptural principles to consider:

- **Seek to keep all of our activities consistent with the mind of Christ.**
  Philippians 4:8:"Finally, brethren, whatsoever things are true, whatsoever things are honest, whatsoever things are just, whatsoever things are pure, whatsoever things are lovely, whatsoever things are of good report; if there be any virtue, and if there be any praise, think on these things."

- **Ensure our use of technology represents Christ well.**
  Philippians 1:27:"Let your conversation [whole lifestyle] *be as it becometh* [in a manner worthy of] *the gospel of Christ."*

Questions to consider when considering technology in the workplace:

- Does it appropriately use resources?
- What is its potential for misuse?
- What are necessary safeguards which should be in place?
- How do I guard my employees against the dangers of this technology?

Steps to consider for increased safety:

- Ensure all devices with internet access have programmable content filters. Unfiltered or unmonitored internet access for employees may allow poor stewardship of time and lead to lost productivity, introduce security threats into a computer network, expose the business to legal liability, and allow use of business computers for inappropriate activities.
- Symantec Web Security, SafeEyes, EtherShield Business from Internet Safety.com, and iPrism Web Security by EdgeWave are examples of internet security suites that allow employers to filter, set usage allowances, and monitor internet usage on computer networks.
- Depending on the complexity of the computer network, a computer consultant may be needed to help find the best way to provide internet filtering/monitoring for the business.
- Create and maintain a business email/internet use policy. An example of such a policy is at the end of this document.

For more information on technology resources, please see www.accounseling.org/technology.

SAMPLE INTERNET USE PLAN FOR BUSINESSES

This technology use plan applies to all employees of this company who have access to computers and the Internet during the course of their business activities. Violation of these directives could result in disciplinary and/or legal action.

Computer, email, and Internet use:

- Employees are expected to use the Internet responsibly and productively. Primary usage of the Internet is for job-related activities. Incidental personal use is permitted.
- All internet data that is composed, transmitted, and/or received by company computers are to be considered as company property.
- The equipment and technology used to access the Internet are company property and the company reserves the right to monitor internet and email traffic.
- Any websites or downloads may be monitored and/or blocked by the company if they are considered harmful and/or not productive to business.
- The personal installation of programs and applications by employees will be monitored.

Unacceptable use of the Internet includes, but is not limited to:

- Sending or posting discriminatory, harassing, threatening, or vulgar messages or images on the Internet or through email.
- Using company computers fraudulently through pirating software, films, or music.
- Stealing, using, or disclosing someone else's password.
- Downloading, copying, or pirating software and electronic files that are copyrighted or without proper authorization.
- Sending confidential material, trade secrets, or proprietary information outside of the company.
- Hacking into unauthorized websites using company computers.
- Purposefully bypassing company monitors and filters.
- Sending or posting information that is defamatory to the company, its employees, products, or customers.
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.
- Passing off personal views as representative of the company.

User compliance:
All terms and conditions as stated in this document are applicable to all users of this company's network and internet connection. I understand and will abide by this Internet Use Policy knowing that any violation thereof could cause my access privileges to be revoked and may result in disciplinary or legal action.

_____ _____

Employee signature Date